



PROCESO DIRECCIONAMIENTO
ESTRATEGICO (Planeación)

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2023

“ITFIP” Institución de Educación Superior



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

Oficina Asesora de Planeación
Grupo Interno de Trabajo Sistemas





**PROCESO DIRECCIONAMIENTO
ESTRATEGICO (Planeación)**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2023**

Versión: 3.0

Página 3 de 7

Fecha: Enero 31 de 2023

**“ITFIP”
INSTITUCIÓN DE EDUCACIÓN
SUPERIOR**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

MARIO FERNANDO DÍAZ PAVA
Rector

LUIS ALBERTO VASQUEZ GUERRA
Asesor de Planeación

Diseño y elaboración:

Luis Alberto Vásquez Guerra

Espinal – Enero 31 de 2023

	PROCESO DIRECCIONAMIENTO ESTRATEGICO (Planeación) PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023	Versión: 3.0
		Página 3 de 7
		Fecha: Enero 31 de 2023

1. OBJETIVO

Describir las actividades que se desarrollarán como parte del plan de Seguridad y Privacidad de la Información, que permitan implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el Instituto Tolimense de Formación Técnica Profesional ITFIP.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información se aplica a todos los procesos del Instituto Tolimense de Formación Técnica Profesional ITFIP, en concordancia con el Sistema Integrado de Gestión y la Política de Seguridad de la Entidad.

3. TÉRMINOS Y DEFINICIONES

- **Ciberseguridad:** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.
- **Información pública:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.
- **Internet:** Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
- **Vulnerabilidad o Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **Seguridad de la información:** Protección de la información y de los sistemas

	PROCESO DIRECCIONAMIENTO ESTRATEGICO (Planeación) PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023	Versión: 3.0
		Página 3 de 7
		Fecha: Enero 31 de 2023

de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

4. MARCO LEGAL

- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- LEY 527 DE 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
- LEY 1474 DE 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
- LEY 1712 DE 2014: por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
- DECRETO 103 DE 2015: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- LEY 1266 DE 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- LEY 23 DE 1982: sobre Derechos de Autor. Congreso de la República.
- CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991: Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Tolimense de Formación Técnica Profesional ITFIP, se compromete a

	PROCESO DIRECCIONAMIENTO ESTRATEGICO (Planeación) PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023	Versión: 3.0
		Página 3 de 7
		Fecha: Enero 31 de 2023

establecer los lineamientos que permitan proteger la Información de la Entidad a través de buenas prácticas del uso de la Información, teniendo en cuenta requisitos legales, operativos, tecnológicos y administrativos; lo anterior, con el fin de asegurar el cumplimiento, disponibilidad, legalidad y confidencialidad de la información.

6. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

- Identificar e implementar lineamientos necesarios para fortalecer la función de la seguridad, privacidad de la información y protección de datos.
- Fortalecer la aplicabilidad de las normativas vigentes sobre seguridad, privacidad de la información y protección de datos.
- Proteger la información y los activos tecnológicos de la entidad, mediante buenas prácticas, recomendaciones y toma de conciencia de la importancia de estas.
- Concientizar a los funcionarios, contratistas, estudiantes, practicantes, y todo el personal que haga parte del Itfip, sobre la importancia de la aplicabilidad de la política de seguridad, privacidad de la información y protección de datos.
- Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Línea respecto a la Seguridad de la Información.

7. ALCANCE DE LA POLÍTICA DE SEGURIDAD

Con la constante actualización de la política de seguridad, privacidad de la información y protección de datos, se pretende poner en funcionamiento dentro de los procesos de la entidad las nuevas normativas impartidas por el Gobierno Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones para entidades de carácter público.

De igual forma, es importante destacar que el objetivo de esta política es brindar las directrices que se deben tener en cuenta para que el resguardo, protección y almacenamiento de información que se genere dentro de la entidad sea conservada de manera correcta.

Haciendo un enfoque más específico, esta política busca capacitar y concientizar a todos los funcionarios del Itfip tanto de planta, carrera administrativa y contratistas, a tomar responsabilidad por toda la información manejada y la importancia que representa la política de seguridad, privacidad de la información y protección de datos para la entidad.

	PROCESO DIRECCIONAMIENTO ESTRATEGICO (Planeación) PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023	Versión: 3.0
		Página 3 de 7
		Fecha: Enero 31 de 2023

8. RESPONSABLE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Oficina Asesora de Planeación y el Grupo Interno de Trabajo de Sistemas, tienen dentro de sus funciones Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

9. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

10. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DESARROLLADAS

Con la implementación de la Política de Seguridad en la Entidad, se han desarrollado actividades hacia el mejoramiento y reducción de la vulnerabilidad o riesgos de seguridad entre las que se encuentran:

- Aprobación por parte de los directivos de la Institución y posterior publicación de la Política de Seguridad y Privacidad de la información, en la página Web del Itfip.
- Capacitación al personal de la Institución en cuanto a los riesgos de seguridad más frecuentes.
- Solicitud formal del porte del carnet institucional.
- Promoción a través del correo institucional de varios Tips de seguridad que los empleados deberán tener en cuenta.
- Mejora en el control de los equipos de cómputo de la Institución.
- Aumento de los controles en el uso del servicio de internet para los funcionarios de la Institución.

11. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2023 se definen las siguientes actividades para reducir los riesgos de seguridad y Privacidad de Información, las cuales se encuentran enmarcadas en el Plan Anticorrupción y de Atención al Ciudadano:



**PROCESO DIRECCIONAMIENTO
ESTRATEGICO (Planeación)**

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2023**

Versión: 3.0

Página 3 de 7

Fecha: Enero 31 de 2023

ACTIVIDAD	RESPONSABLE	FECHA
Realizar la actualización de la política de seguridad, privacidad de la información y protección de datos.	Oficina Asesora de Planeación	31 de enero 2023
Continuar con la promoción de la política de seguridad, privacidad de la información y protección de datos a todos los funcionarios de la Institución (contratistas y funcionarios de planta, además realizar la respectiva implementación de ésta.	Oficina Asesora de Planeación/ Área de Sistemas	Durante toda la vigencia
Gestionar para que en la entidad se realice la actualización y clasificación de los activos de información y sobre los cuales se definieron acciones de mitigación de riesgos.	Oficina Asesora de Planeación/ Área de Sistemas	Marzo del 2023
Implementar una estrategia para administrar y actualizar los activos de información (equipos de cómputo y de comunicaciones) promoviendo en especial la utilización de contraseñas apropiadas según la política de seguridad y privacidad de la entidad.	Oficina Asesora de Planeación/ Área de Sistemas	Durante toda la vigencia
Evaluar la importancia de los activos de información que se manejen en cada una de las dependencias de los líderes de procesos para posteriormente proceder a realizar y almacenar de manera segura los backup que sean necesarios.	Delegado de cada dependencia/Oficina Asesora de Planeación	Abril del 2023